In today's environment, we are seeing a major shift toward multi-cloud infrastructure. This is where organizations use public or private cloud services, often in combination with hybrid cloud, or rely on multiple cloud providers to deliver business services. The main driver behind this shift is that many businesses no longer want the responsibility of maintaining traditional networking equipment or being responsible for reliability issues, hardware failures, and system replacements. They feel that by moving to the cloud, they will save money on staffing, equipment, building space, and maintenance. What they need to keep in mind is that as they move into cloud and hybrid cloud environments, their security requirements increase. They now need continuous, policy driven, automated controls to keep these cloud environments secure.

In a traditional enterprise setup, organizations owned their data centers and all the equipment inside them. In a multi-cloud environment, workloads are spread across different providers, and companies try to combine the strengths of each. For example, AWS may excel at certain services, while Azure may be a better choice for SQL based workloads because it aligns with Microsoft's ecosystem. A major misconception business often have is that moving to the cloud eliminates their security responsibilities. That is not the case. The responsibility increases because organizations still must properly configure these platforms and employ people who understand how these environments work.

Identity management becomes a challenge as companies adopt multi-cloud. Access must be configured correctly, and as the environment changes, configurations must be updated accordingly. Any change can introduce new vulnerabilities. Another challenge is maintaining compliance across all providers. If a business must follow a certain standard, every cloud provider they use must be capable of meeting those compliance requirements.

Multi-cloud also brings real advantages. One major benefit is avoiding vendor lock in. Companies are not trapped with a single provider and can shift workloads if prices rise or service declines. Multi-cloud also helps with geographic presence and regulatory compliance. If a business operates in multiple countries, it can use cloud providers in those regions knowing they support local regulations, such as GDPR. Multi-cloud setups can also offer cost flexibility, since spreading workloads across providers may allow organizations to take advantage of better pricing models.

At the same time, multi-cloud increases complexity and the overall attack surface. Each provider has its own tools and interfaces, making it harder to hire staff who know all of them. More clouds mean more services, more configurations, and more opportunities for misconfigurations. Another complication is data movement between providers. Not all clouds communicate well, and differences in protocols or services can create problems and cause compatibility challenges.

Overall, multi-cloud and hybrid cloud environments come with both advantages and challenges. As security professionals, we need to make sure our C-suite understands exactly what the business is getting into before committing to a multi-cloud strategy. It is our responsibility to clearly explain both the benefits and the risks so leaders can make informed decisions and fully understand the impact this will have on security and operations.

References:

https://www.tripwire.com/state-of-security/multi-cloud-security-best-practices-guide

https://www.legitsecurity.com/aspm-knowledge-base/multi-cloud-security

https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/multi-cloud-security